

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

1-31. Canceled.

32. (Currently Amended) A transparent encryption appliance that does not store data for protecting data received from the ~~a web stored in a database~~ by a web server environment that ~~does not secure by encrypting, hashing, or keyed hashing the data received from the web before it is stored~~, the transparent encryption appliance comprising:

at least one client network interface for coupling to at least one network and communicating with one or more clients via the at least one network;

a server interface for coupling to a web server environment;

wherein that does not include the appliance is separate from the web server environment and is operative to be connected between the web server environment and the at least one network, wherein the server interface and the at least one client network interface communicate using the same communications protocol; and

a processor coupled to the at least one client network interface and the server interface for at least one of securing and unsecuring data, wherein:

securing data comprises: evaluating identifying first sensitive data contained in a data transaction received through the at least one client network interface; identifying first sensitive data contained in said data transaction; securing only the sensitive data by at least one of encrypting, hashing, and keyed hashing; replacing in the data transaction the identified sensitive data with the secured sensitive data; and providing the data transaction including the secured sensitive data through to the web server environment, wherein the secured sensitive data is stored in a database by the web server environment interface; and

unsecuring data comprises: responsive to a request received through the at least one client network interface for sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data, receiving through from the web server interface environment the secured sensitive data corresponding to the requested data

~~retrieved from a database by the web server environment; unsecuring the received secured data by at least one of decrypting and hash verifying; and providing the unsecured sensitive data through the at least one client network interface.~~

33. (Currently amended) The appliance of claim 32, wherein:
in securing data the data transaction is received through a first said client interface; and
in unsecuring data the request is received, and the unsecured data is provided through, the first said client interface or a second said client interface.

34. (Previously Presented) The appliance of claim 32, wherein the processor manages SSL traffic and handles computations that support SSL connections, wherein at least one of:

in securing data the data transaction is received via a first SSL connection and SSL computations are completed before identifying the first sensitive data contained in the data transaction; and

in unsecuring data the unsecured data is provided via a second SSL connection.

35. (Previously Presented) The appliance of claim 32, wherein the received data transaction is one of a cleartext transaction and a Hypertext Transfer Protocol (HTTP) transaction.

36. (Previously Presented) The appliance of claim 32, wherein the at least one network is at least one of the Internet, a wired network type, a wireless network type, a hybrid network type, an independent network, a proprietary network, or a back plane network.

37. (Previously Presented) The appliance of claim 32, further comprising a key storage for storing at least one cryptographic key for use in at least one of the securing and unsecuring of data.

38. (Previously Presented) The appliance of claim 37, further comprising a user interface for use in loading the at least one key into the key storage.

39. (Previously Presented) The appliance of claim 38, wherein the user interface is further for use in specifying access controls to the stored keys.

40. (Previously Presented) The appliance of claim 32, further comprising a user interface for use in specifying one or more fields containing the sensitive data.

41. (Previously Presented) The appliance of claim 40, wherein the one or more fields are identified by one or more regular expressions.

42. (Currently Amended) The appliance of claim 32, wherein the appliance secures and unsecures web cookies provided by the web server environment, wherein:

securing a cookie comprises: identifying a cookie received through the server interface; securing the cookie by at least one of encrypting, hashing, and keyed hashing the cookie; and providing the secured cookie to one of the one or more clients through the at least one client network interface without providing means to the client to unsecure the cookie, wherein the secured cookie is stored in the client; and

unsecuring the cookie comprises: responsive to a request received through the server interface for the cookie stored on a client, receiving from the client the secured cookie corresponding to the requested cookie through the at least one client network interface; unsecuring the received secured cookie by at least one of decrypting and hash verifying; and providing the unsecured cookie through the server interface.

43. (Canceled)

44. (Currently Amended) A system for protecting data stored in a web server environment, comprising:

at least one client coupled to at least one network;

a web server environment that stores data received from the web in at least one database and does not secure by encrypting, hashing, or keyed hashing the data received from the web before it is stored; and

a transparent encryption appliance separate from the web server environment and connected between the web server environment and said at least one network that does not store data for protecting the data stored in the web server environment, comprising:

at least one client network interface coupled to the at least one network and communicating with the at least one client via the at least one network;

a server interface coupled to the web server environment, wherein the server interface and the at least one client network interface communicate using the same communications protocol; and

a processor coupled to the at least one client network interface and the server interface for at least one of securing and unsecuring data, wherein:

securing data comprises: inspecting identifying first sensitive data contained in a data transaction received through the at least one network interface; identifying first sensitive data contained in said data transaction; securing only the first sensitive data by at least one of encrypting, hashing, and keyed hashing; replacing in the data transaction the identified first sensitive data with the secured sensitive data; and providing the data transaction including the secured first sensitive data to the web server environment, wherein the secured first sensitive data is stored in said at least one [[a]] database by the web server environment; and

unsecuring data comprises: responsive to a request received through the at least one network interface for sensitive data corresponding to at least a portion of the stored secured first sensitive data or other stored secured sensitive data, receiving from the web server environment the secured sensitive data corresponding to the requested data retrieved from said at least one [[a]] database by the web server environment; unsecuring the received secured data by at least one of decrypting and hash verifying; and providing the unsecured sensitive data through the at least one client network interface.

45. (Previously Presented) The system of claim 44, wherein the processor of the appliance manages SSL traffic and handles computations that support SSL connections, wherein at least one of:

in securing data the data transaction is received via a first SSL connection and SSL computations are completed before identifying the first sensitive data contained in the data transaction; and

in unsecuring data the unsecured data is provided via a second SSL connection.

46. (Previously Presented) The system of claim 44, wherein the data transaction received by the appliance is one of a cleartext transaction and a Hypertext Transfer Protocol (HTTP) transaction.

47. (Previously Presented) The system of claim 44, wherein the appliance further comprises a key storage for storing one or more cryptographic keys for use in at least one of the securing and unsecuring of data.

48. (Previously Presented) The system of claim 47, wherein the appliance further comprises a user interface for use in loading the one or more keys into the key storage and specifying access controls to the stored one or more keys.

49. (Previously Presented) The system of claim 44, wherein the appliance further comprises a user interface for use in specifying one or more fields containing the sensitive data, wherein the one or more fields are identified by one or more regular expressions.

50. (Currently amended) The system of claim 44, wherein the appliance further secures and unsecures web cookies provided by the web server environment, wherein:

securing a cookie comprises: identifying a cookie received through the server interface; securing the cookie by at least one of encrypting, hashing, and keyed hashing the cookie; and providing the secured cookie to one of the one or more clients through the at least one client network interface without providing means to the client to unsecure the cookie, wherein the secured cookie is stored in the one client; and

unsecuring the cookie comprises: responsive to a request received through the server interface for the cookie, receiving the secured cookie corresponding to the requested cookie through the at least one client network interface; unsecuring the received secured cookie by at least one of decrypting and hash verifying; and providing the unsecured cookie through the server interface.

51. (Canceled)

52. (Currently Amended) A system for protecting stored passwords ~~stored in a web server environment~~, comprising:

one or more clients coupled to at least one network;

a web server environment that stores data received from the web and does not secure by encrypting, hashing, or keyed hashing the data received from the web before it is stored; and

a transparent encryption appliance separate from the web server environment and connected between the at least one network and the web server environment and operative to protect for proteeting passwords contained in the data stored in the web server environment, comprising:

at least one client network interface coupled to the at least one network and communicating with the one or more clients via the at least one network;

a server interface coupled to the web server environment, wherein the server interface and the at least one client network interface communicate using the same communications protocol; and

a processor coupled to the at least one client network interface and the server interface for securing passwords, wherein securing a password comprises identifying a password contained in a data transaction received through the at least one client network interface; securing the password by at least one of encrypting, hashing, and keyed hashing, while not securing the transaction as a whole; replacing in the data transaction the identified password with the secured password; and providing the data transaction including the secured password to the web server environment;

wherein, responsive to a request received through the at least one client network interface of the appliance for an action requiring authorization and containing a password, the appliance secures the password contained in the request, while not securing the request as a whole, and provides the request including the secured password to the web server environment; the web server environment obtains the secured password from the provided data transaction request, retrieves a secured password previously secured by the appliance and stored by the web server, compares the obtained secured password to the retrieved previously stored secured password,

and authenticates the action requiring authorization in the case the obtained secured password matches the retrieved previously stored secured password.

53. (Currently Amended) A method of protecting data stored in a web server environment that does not secure data by encrypting, hashing, or keyed hashing, comprising:

receiving from a client by a transparent encryption appliance that does not store data a data transaction containing sensitive data, the transparent encryption appliance being separate from the web server and connected between the client and the web server;

identifying the sensitive data;

securing only the identified sensitive data by at least one of encrypting, hashing, and keyed hashing;

replacing in the data transaction the identified sensitive data with the respective secured sensitive data; and

providing the data transaction with the secured sensitive data to the [[a]] web server that does not secure data by encrypting, hashing, or keyed hashing; and

storing the provided secured sensitive data in a database by the web server.

54. (Previously presented) The method of claim 53, further comprising after the storing step:

responsive to a request for at least a portion of the sensitive data, retrieving from the database by the web server the stored secured sensitive data corresponding to the requested sensitive data;

forwarding the retrieved secured sensitive data to the transparent encryption appliance;

unsecuring the retrieved sensitive data by at least one of decrypting and hash verifying;

and

providing the unsecured sensitive data to fulfill the request.

55. (Currently Amended) A computer readable storage medium storing executable instructions which, when executed in a computer, protect sensitive information stored in a web server environment by a method comprising:

receiving by a transparent encryption appliance that does not store data a data transaction containing sensitive data;

identifying the sensitive data;

securing only the identified sensitive data by at least one of encrypting, hashing, and keyed hashing;

replacing in the data transaction the identified sensitive data with the respective secured sensitive data;

providing the data transaction with the secured sensitive data to a web server separate from the transparent encryption appliance that does not secure data by encrypting, hashing, or keyed hashing;

~~storing the provided secured sensitive data in a database by the web server;~~

~~responsive to a request for at least a portion of the sensitive data, receiving at the transparent encryption appliance retrieving from the database by the web server the stored secured sensitive data corresponding to the requested sensitive data;~~

~~forwarding the retrieved secured sensitive data to the transparent encryption appliance;~~

unsecuring the retrieved sensitive data by at least one of decrypting and hash verifying;
and

providing the unsecured sensitive data to fulfill the request.

56. (New) A computer readable storage medium according to claim 55, further comprising a computer readable storage medium storing executable instructions which, when executed in a computer of a web server that does not secure data by encrypting, hashing, or keyed hashing, cause said web server to:

receive the data transaction with the secured sensitive data from the transparent encryption appliance;

store the provided secured sensitive data in a database;

responsive to a request for at least a portion of the sensitive data, retrieve from the database the stored secured sensitive data corresponding to the requested sensitive data; and

forward the retrieved secured sensitive data to the transparent encryption appliance to be unsecured.